IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, October 2025
Impact Factor: 7.67

An Analytical Survey on Certificate-Less Cryptography Techniques for Ensuring Cloud Data Integrity through Public Auditing

Prof. Dhage S. A.[1], Miss. Arti Sanjay Gore[2],
Miss. Ankita Manohar Kasare[3], Mr. Rushikesh Popat Hajare[4]
[1]Student, Department of Computer Engineering
[2,3,4]Assistant Professor, Department of Computer Engineering
Vishwabharti Academy's College of Engineering, Ahilyanagar, (MH) India
Savitribai Phule Pune University, Pune (MH) India

Abstract: *There is an increasing need to guarantee data integrity in group-shared environments due to the proliferation of cloud computing as a means of collaborative data storage. While Public Key Infrastructure (PKI) is effective, it adds complexity and administrative overhead to traditional integrity testing methods owing to certificate administration. In order to validate group-shared data on cloud platforms without requiring certificates, this project suggests a certificate-less public integrity-checking mechanism. The protocol efficiently manages keys by utilizing certificate-less cryptography, which reduces computational and storage overhead without compromising security. While maintaining confidentiality, authorized group members or external auditors can confirm data integrity without gaining direct access to the data. Protocol features also include dynamic group administration, which makes it easy to add or remove members without affecting data integrity. A scalable and efficient alternative for public integrity verification in cloud-based collaborative environments, experimental results show that this certificate-less technique delivers equivalent or superior performance over existing PKI-based systems.*

Keywords*:* Cloud storage security, group-shared data, Certificate-less cryptography, public integrity checking, data integrity verification

DOI: 10.48175/IJARSCT-29380